Experimental verification of quantum computations

Experimental verification of quantum computations

Stefanie Barz[1], Joseph F. Fitzsimons[2,3], Elham Kashefi[4], Philip Walther[1]
[1] *University of Vienna, Faculty of Physics, Boltzmanngasse 5, 1090 Vienna, Austria,*
[2] *Singapore University of Technology and Design, 20 Dover Drive, Singapore 138682,*
[3] *Centre for Quantum Technologies, National University of Singapore, Block S15, 3 Science Drive 2, Singapore 117543,*
[4] *School of Informatics, University of Edinburgh, 10 Crichton Street, Edinburgh EH8 9AB, UK*

Quantum computers are expected to offer substantial speedups over their classical counterparts and to solve problems that are intractable for classical computers. Beyond such practical significance, the concept of quantum computation opens up new fundamental questions, among them the issue whether or not quantum computations can be certified by entities that are inherently unable to compute the results themselves. Here we present the first experimental verification of quantum computations. We show, in theory and in experiment, how a verifier with minimal quantum resources can test a significantly more powerful quantum computer. The new verification protocol introduced in this work utilizes the framework of blind quantum computing and is independent of the experimental quantum-computation platform used. In our scheme, the verifier is only required to generate single qubits and transmit them to the quantum computer. We experimentally demonstrate this protocol using four photonic qubits and show how the verifier can test the computer's ability to perform measurement-based quantum computations.

The prevalent scientific paradigm of testing physical theories by comparing experimental results with predictions computed on a piece of paper or on a computer assumes that all such predictions are solvable in polynomial time on a classical computer. In current experiments involving quantum particles, such as fundamental tests of quantum mechanics or small-scale quantum computations and simulations [1–5], following this paradigm is still possible, as the results can be calculated on a classical computer and verified in experiments involving quantum systems. However, there is an entire class of problems—for example, the simulation of complex quantum systems [6]—that are solvable in polynomial time only on a quantum computer [7].

One of the central conceptual questions in current quantum computing is therefore whether any entity can test the results obtained by a quantum computer, even when that entity is unable to compute these results itself. Or, from a different perspective, can an experimentalist with only classical resources or restricted quantum resources prove that a given device is a quantum computer [8]? Whereas the ultimate answer to such questions is still open, there are several proposals that offer a solution when the verifier is equipped with a range of quantum resources [9–14]—quantum memory, two entangled quantum computers, or a large number of qubits—which, however, are outside the reach of current technology.

Here, we demonstrate how to verify a quantum computation on four qubits. Our method is directly applicable to current technology and can be readily extended to more general cases. We show that only minimal quantum resources (specifically, single qubits) are required to certify a quantum-information processor. Our protocol is independent of the physical system on which it is implemented and it can therefore be applied to any quantum-computing platform.

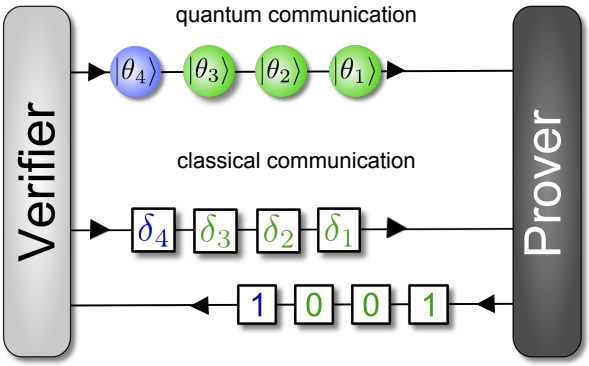


FIG. 1: Concept of a quantum prover interactive proof system based on blind quantum computing. The verifier wants to find out if the prover can indeed perform quantum computations. While the question of whether a classical verifier can test a quantum system is still open, it was shown that a verifier who has access to certain quantum resources can verify quantum computations. Here, in the framework of blind quantum computing, the verifier has to be able to generate single qubits and to transmit them to the prover. After the transmission of the qubits, the verifier and the prover exchange two-way classical communication.

We have implemented the new protocol on a photonic quantum system and demonstrate the necessary components for verifying a quantum device. We also show how our scheme can be used to verify the generation of the archetype of a quantum-computational resource, quantum entanglement, via a violation of Bell's inequality. In such a verification, the prover remains blind and cannot distinguish the verification procedure from standard quantum-computational tasks such as single- or multi-qubit gates or entire quantum algorithms. To the best

of our knowledge, this is the first experiment towards certifying the correctness of a quantum computation.

INTERACTIVE PROOF SYSTEMS AND BLIND QUANTUM COMPUTING

Our protocol combines interactive proof systems and blind quantum computing [9–11]. Interactive proof systems were originally invented in the field of computer science, to approach questions in classical complexity theory [15, 16]. They have since been extended into the realm of quantum computation [7]. A *quantum prover interactive proof* system addresses the question of whether a prover who has access to quantum-computational resources can convince a classical verifier that he can solve a given problem. Interactive proof systems can therefore be used to address the fundamental questions posed above, provided the traditional scientific paradigm of "predicting" is replaced by "verifying".

In our protocol, the framework of the interactive proof system is given by blind quantum computing (Fig. 1). In this framework, a verifier (or client) with limited quantum computational resources can delegate a quantum computation to a prover (or server) with the full power of quantum computing such that all data and the whole computation remain private [10, 17]. More specifically, the verifier prepares single qubits in the state

$$|\theta_j\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + e^{i\theta_j}|1\rangle\right) \tag{1}$$

with $\theta_j \in \{0, \pi/4, ..., 7\pi/4\}$ chosen uniformly at random and only known to the verifier. The qubits are then transmitted to the prover who entangles them to create a blind cluster state [18]. The actual computation is measurement-based [19, 20]. The verifier calculates for each blind qubit measurement instructions according to

$$\delta_j = \theta_j + \phi_j + \pi r_j \tag{2}$$

where θ_j is the blind phase of the qubit, ϕ_j is the rotation that the verifier wants to perform (including any Pauli corrections), and $r_j \in \{0, 1\}$ is a randomly chosen value to hide the measurement outcome. The prover performs measurements in the basis

$$|\pm_{\delta_j}\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle \pm e^{i\delta_j}|1\rangle\right) \tag{3}$$

and delivers the results to the verifier. Without the knowledge of the underlying rotation and the random phase, the prover cannot find out anything about the actual rotation ϕ_j—thus the computation remains blind. The verifier, in contrast, knows the initial rotation and is able to interpret the results. Blind quantum computing therefore provides a powerful tool to delegate computations and to access the resources of powerful quantum computers without divulging the content of the computation. In the following, we show how this concept can be applied to verify quantum computations.

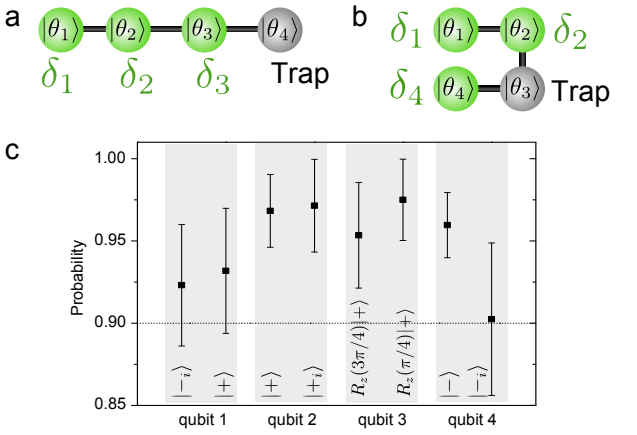


FIG. 2: Measurement verification. a,b) A blind linear cluster state and a blind rotated horseshoe cluster state which can be used for the preparation of trap qubits. c) Experimental results of the measurement verification. We prepare two different trap state on each qubit 1-4 and show the probability of obtaining the correct outcome when measuring those qubits.

VERIFICATION OF A QUANTUM COMPUTATION

In the framework of blind quantum computing, in order to test a quantum computation, the correctness of the measurements performed by the server has to be verified. Here we use a verification procedure that is based on the creation of trap qubits [12]. Trap qubits are blindly prepared in a well-defined state, which is only known to the verifier, and are isolated from the actual computation. The measurement angle of these trap qubits is chosen such that the measurement result is predetermined by the verifier, and hence any cheating strategy used by the server that alters these measurement outcomes will be detected. By randomly choosing the locations of the trap qubits it is then possible to bound the probability that the server can cheat while remaining undetected.

In our setting, we implement the preparation of the trap qubits through a measurement-based computation on the non-trap qubits. The verifier chooses measurement settings on the cluster state such that any of the qubits could become a trap qubit, prepared in a random state $|\theta_j\rangle$. If the trap qubit is then measured in the basis $|\theta_j\rangle$, the outcome will always be known to the verifier (see Fig. 2). Our measurement-based creation of the trap qubits means that we verify a correlation between a subset of measurements, rather than a single measurement outcome. We therefore have to be careful to ensure that the correctness of these correlations for all trap measure-

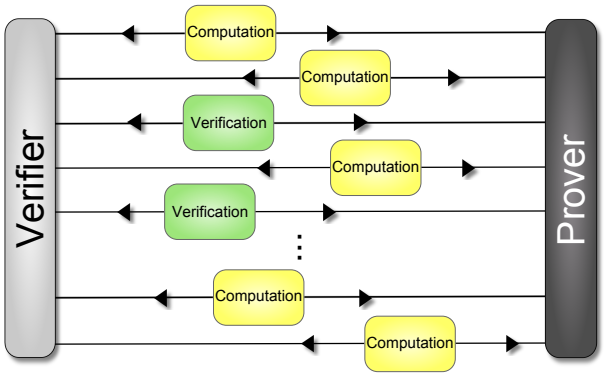


FIG. 3: Schematic of a quantum computation with verification sub-routines.

ments does imply the correctness of a given computational run. In our demonstration using a four-qubit system, only one error remains undetected (see Appendix). However, this particular error cannot alter the result of the measurement of Bell's quantity presented in this paper.

This verification procedure can be used to verify that the quantum computation was performed correctly. Therefore, we consider multiple runs of the protocol, where the verifier randomly choses to run an actual computation or a verification test (see Fig. 3). This use of multiple runs of the blind-computation protocol lets us make optimal use of the qubits available in our system. Moreover, the server cannot distinguish between an actual computation run or a trap run. Hence, as discussed in details in the appendix, this procedure can be used to verify not only the correctness of the measurement outcomes but also of the entire quantum computation. When trap computation and target computation are randomly interspersed, then the probability that the quantum computer produces the correct result for the verification runs but a wrong result for the computation runs is bounded by a value depending on three parameters: the number of computation runs, the number of trap runs, and on the total number of qubits in the system (see appendix).

ENTANGLEMENT VERIFICATION

Once the measurement outcomes are verified, we can proceed to use the system to probe the prover's entangling capabilities and its ability to create cluster states. Quantum correlations are typically confirmed by well-established tests of Bell's inequality [21] (Fig. 4). In order to do so, combinations of specific measurement settings α, α' and β, β' are performed on the first (a) and on the second qubit (b), respectively, after generating an entangled state $|\Psi\rangle_{a,b}$. The settings are chosen such that a maximal violation of the Bell inequality of the Clauser-

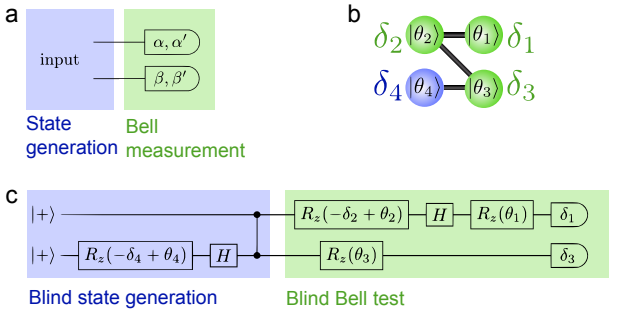


FIG. 4: A blind Bell test for the verification of quantum resources. a) Conventional scheme for a Bell test, where first an (entangled) state is created and then Bell measurements are performed. b) The blind zigzag cluster state, and c) its corresponding circuit. If the rotation in the lower wire, $-\delta_4+\theta_4$, is chosen equal to zero (or π), the input state in the lower wire will be equal to $|0\rangle_b$ ($|1\rangle_b$); otherwise, if the rotation is chosen equal to $\pm\pi/2$ the input will be $|\pm_i\rangle_b$. The edge between qubits 2 and 3 performs a CPhase gate on the two qubits, which results in an entangled state in the former case, and in an unentangled state in the latter. The values of δ_1, δ_2, and δ_3, as well as the phases θ_1, θ_2, and θ_3 determine the Bell measurement settings.

Horne-Shimony-Holt (CHSH) type [22] is obtained for an entangled state:

$$S = |E(\alpha,\beta) - E(\alpha,\beta')| + |E(\alpha',\beta) + E(\alpha',\beta')| \leq 2 \quad (4)$$

The correlation coefficients $E(\cdot,\cdot)$ are defined by the coincidence counts when measuring qubit a in the basis α and qubit b in the basis β (for details see appendix).

In order to make the Bell test blind, we hide the generation of the entangled state as well as the Bell measurement settings. For this, we base our implementation on a blind zigzag cluster state with four qubits $|\theta_j\rangle$, which is shown in Fig. 4b. Single-qubit measurements on the blind zigzag cluster state realize a quantum circuit that offers exactly the degrees of freedom that are necessary for our blind Bell test. First, using this type of cluster, the verifier has the possibility to blindly switch between entangled or separable input states by choosing δ_4 and θ_4 accordingly. Second, the standard measurement settings for a Bell test are hidden as they are determined by the phases of the blind qubits $|\theta_1\rangle$, $|\theta_2\rangle$, and $|\theta_3\rangle$ and their respective measurement settings of δ_1, δ_2, and δ_3 (see appendix for details).

As a result, the state generation as well as the Bell-state measurements are encoded in the phase of blind qubits as well as in the measurement instructions, which remain unknown to the prover at any time. The choice of the cluster-state configuration also remains hidden from the prover. This is a particular advantage of our probabilistic implementation of blind quantum computing, where all qubits are measured.

EXPERIMENT

We use the particular advantages offered by photons to realize a quantum network that can communicate and process quantum information [23] within the same physical system [18]. In our experiment, the blind cluster states are generated from photon pairs entangled in polarization and mode, which originate from spontaneous parametric down-conversion [24]. Our setup and the methods used are explained in detail in ref. 10; in the present experiment, we generate blind cluster states for various settings of θ_j and use them to implement exemplary runs of trap computations as well as the Bell-test runs—the necessary building blocks of a verified test of Bell's quantity.

For the demonstration of the measurement verification, we use blind linear cluster states and blind rotated horseshoe cluster state to prepare traps as shown in Fig. 2a and 2b. By choosing the blind phases θ_j and measurement settings δ_j as given in the appendix, we prepare the traps:

$$|\mathrm{trap}_1\rangle = |-_i\rangle \text{ and } |+\rangle \quad (5)$$
$$|\mathrm{trap}_2\rangle = |+\rangle \text{ and } |+_i\rangle \quad (6)$$
$$|\mathrm{trap}_3\rangle = R_z(3\pi/4)|+\rangle \text{ and } R_z(\pi/4)|+\rangle \quad (7)$$
$$|\mathrm{trap}_4\rangle = |-\rangle \text{ and } |-_i\rangle \quad (8)$$

on qubits 1, 2, 3, and 4, respectively ($|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$, $|\pm_i\rangle = (|0\rangle \pm i|1\rangle)/\sqrt{2}$). The probabilities to find the correct outcome are well above 90%, as shown in Fig. 2c.

For a verification of quantum entanglement, we choose combinations of θ_4 and δ_4 to create the entangled state:

$$|\Psi\rangle_{a,b} = \frac{1}{\sqrt{2}}(|+\rangle_a|0\rangle_b - i|-\rangle_a|1\rangle_b) \quad (9)$$

and to blindly implement the Bell measurements settings we choose:

$$\alpha = \pi/2, \;\; \alpha' = \sigma_z, \;\; \beta = -3\pi/4, \;\; \beta' = -\pi/4 \quad (10)$$

where the bases α, β, and β' are defined as $\{(|0\rangle \pm e^{i\alpha}|1\rangle)/\sqrt{2}\}$ etc., and α' is a measurement in the basis $\{|0\rangle, |1\rangle\}$. To obtain the measurement settings given in Eq. (10), we choose combinations of $|\theta_j\rangle$ and δ_j as given in detail in the appendix. From the measured coincidence count rates, we calculate the correlation coefficients to be:

$$E(\alpha,\beta) = -0.540 \pm 0.084 \quad (11)$$
$$E(\alpha,\beta') = 0.634 \pm 0.086 \quad (12)$$
$$E(\alpha',\beta) = -0.646 \pm 0.067 \quad (13)$$
$$E(\alpha',\beta') = -0.678 \pm 0.079. \quad (14)$$

Those coefficients lead to an S parameter of

$$S = 2.498 \pm 0.158, \quad (15)$$

which violates the classical bound ($|S| = 2$) by more than 3 standard deviations.

The combination of the verification procedure and this violation of Bell's inequality suffices to unambiguously verify the prover's ability to perform entangling gates between qubits and thus to create cluster states. In our experiment, we implement a subset of all possible blind states. The states of qubits 1 and 4 are fixed to $|+\rangle$, whereas the states of qubits 2 and 3 are fully blind [18]. The whole verification procedure remains blind, however, if we assume that the prover has no *a priori* knowledge of our choice of states and measurements.

The violation of Bell's inequalities is impossible classically, not for the reason of high complexity, but rather on the basis of physical principles. In our implementation, we assume the correctness of quantum mechanics for the verification of the measurement outcomes. Without this assumption, a full demonstration would require the two entangled photons to be sent to two distant laboratories, where only at the very last step of the computation the verifier gives the measurement instructions to the prover. In this way, no classical computer could mimic, even in principle the output of the computation *a priori*, while the verification procedure would still have a positive outcome.

CONCLUSION

Future large-scale quantum computers and quantum simulators [25–28] will require the verification of their experimental results [29]. Due to the superior computational capacity of quantum systems the results cannot simply be calculated and checked on a classical device. The development of new methods for the verification of quantum computations is therefore a crucial task. Here, we have developed a new general method for verifying quantum computations that can be readily applied to current small-scale quantum computers. We have shown, in theory and in experiment, how a verifier can test whether the quantum computer is quantum and even whether it computes correctly.

Finally, how verification mechanisms provide insights into questions of computational complexity and into the foundations of quantum physics it is a topic of active current research. To date, the limit of high computational complexity is mostly unexplored and it is not impossible that quantum mechanics breaks down at some scale of complexity [30].

Verification methods, such as those reported here in are not only important as a mechanism to certify quantum computers, but also provides an entirely novel toolbox for addressing fundamental questions in quantum physics and computer science.

[1] D. Deutsch, Proc. R. Soc. A **400**, 97 (1985).
[2] D. Deutsch and R. Jozsa, Proc. R. Soc. A **439**, 553 (1992).
[3] L. K. Grover, in *Proceedings of the 28th Annual ACM Symposium on the Theory of Computing* (1996), pp. 212–219.
[4] P. W. Shor, SIAM J. Comput. **26**, 1484 (1997).
[5] A. W. Harrow, A. Hassidim, and S. Lloyd, Phys. Rev. Lett. **103**, 150502 (2009).
[6] R. Feynman, Int. J. Theor. Phys. **21**, 467 (1982).
[7] J. Watrous, arXiv:0804.3401 (2008).
[8] A. Pappa, A. Chailloux, S. Wehner, E. Diamanti, and I. Kerenidis, Phys. Rev. Lett. **108**, 260502 (2012).
[9] D. Aharonov, M. Ben-Or, and E. Eban, arXiv:0810.5375 (2008).
[10] A. Broadbent, J. Fitzsimons, and E. Kashefi, in *Proceedings of the 50th Annual Symposium on Foundations of Computer Science* (2009), pp. 517–526.
[11] D. Aharonov and U. Vazirani, arXiv:1206.3686 (2012).
[12] J. Fitzsimons and E. Kashefi, arXiv:1203.5217 (2012).
[13] T. Morimae, arXiv:1208.1495 (2012).
[14] B. Reichardt, F. Unger, and U. Vazirani, Nature **496**, 456 (2013).
[15] L. Babai, in *Proceedings of the seventeenth annual ACM symposium on Theory of computing* (ACM, 1985), pp. 421–429.
[16] S. Goldwasser, S. Micali, and C. Rackoff, SIAM J. Comput. **18**, 186 (1989).
[17] T. Morimae and K. Fujii, Nat. Commun. **3**, 1036 (2012).
[18] S. Barz, E. Kashefi, A. Broadbent, J. Fitzsimons, A. Zeilinger, and P. Walther, Science **335**, 303 (2012).
[19] R. Raussendorf and H. Briegel, Phys. Rev. Lett. **86**, 5188 (2001).
[20] R. Raussendorf, D. E. Browne, and H. J. Briegel, Phys. Rev. A **68**, 022312 (2003).
[21] J. Bell, Physics **1**, 195 (1964).
[22] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Phys. Rev. Lett. **23**, 880 (1969).
[23] E. Knill, R. Laflamme, and G. J. Milburn, Nature **409**, 46 (2001).
[24] P. G. Kwiat, K. Mattle, H. Weinfurter, A. Zeilinger, A. V. Sergienko, and Y. Shih, Phys. Rev. Lett. **75**, 4337 (1995).
[25] C. Weitenberg, M. Endres, J. Sherson, M. Cheneau, P. Schauß, T. Fukuhara, I. Bloch, and S. Kuhr, Nature **471**, 319 (2011).
[26] R. Islam, E. Edwards, K. Kim, S. Korenblit, C. Noh, H. Carmichael, G. Lin, L. Duan, C. Wang, J. Freericks, et al., Nature Commun. **2**, 377 (2011).
[27] T. Monz, P. Schindler, J. Barreiro, M. Chwalla, D. Nigg, W. Coish, M. Harlander, W. Hänsel, M. Hennrich, and R. Blatt, Phys. Rev. Lett. **106**, 130506 (2011).
[28] J. Britton, B. Sawyer, A. Keith, C. Wang, J. Freericks, H. Uys, M. Biercuk, and J. Bollinger, Nature **484**, 489 (2012).
[29] D. Leibfried, Nature **463**, 608 (2010).
[30] S. Aaronson, in *Proceedings of the 36th annual ACM Symposium on Theory of Computing* (2004), pp. 118–127, .

Acknowledgment The authors are grateful to S. Aaronson, D. Aharonov, C. Brukner, A. Zeilinger, and F. Verstraete for discussions. S.B. and P.W. acknowledge support from the European Commission, Q-ESSENCE (No. 248095), QUILMI (No. 295293) and the ERA-Net CHISTERA project QUASAR, the John Templeton Foundation, the Vienna Center for Quantum Science and Technology (VCQ), the Austrian Nano-initiative NAP Platon, the Austrian Science Fund (FWF) through the SFB FoQuS (No. F4006-N16), START (No. Y585- N20) and the doctoral programme CoQuS, the Vienna Science and Technology Fund (WWTF) under grant ICT12-041, and the Air Force Office of Scientific Research, Air Force Material Command, United States Air Force, under grant number FA8655-11-1-3004. J.F. acknowledges support from the National Research Foundation and the Ministry of Education, Singapore. E.K. acknowledges support from UK Engineering and Physical Sciences Research Council (EP/E059600/1).

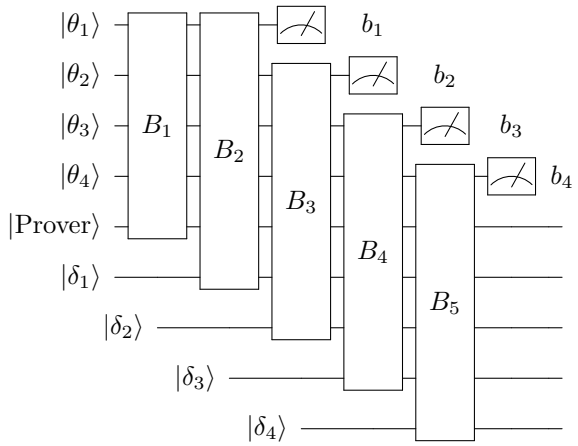
APPENDIX

VERIFICATION OF A QUANTUM COMPUTATION

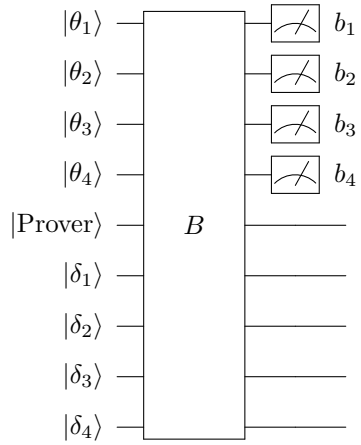
In order to verify a blind quantum computation, it is necessary to ensure that the probability of an undetected error being introduced to the computation is bounded. One way to do this is to introduce trap qubits into the computation as in [12]. To prove that this does in fact guarantee that any error is either detected or corrected except with bounded probability, we must consider the most general possible cheating strategy for the prover. Thus we must consider the effect of an arbitrary deviation at each step of the protocol. In this section we present a simplified version of the proof in [12] adapted to our 4-qubit protocol with classical inputs and outputs, and then show how it can be adapted to work with traps prepared by measurement-based computation.

Individual trap qubits

We assume the most general scenario. The prover obtains the quantum states $|\theta_i\rangle$ and the states $|\delta_i\rangle$ which encode the classical angles δ_i. Further, the prover has access to a private quantum memory $|\text{Prover}\rangle$, where the prover could store quantum information allowing him to perform the most general attacks:

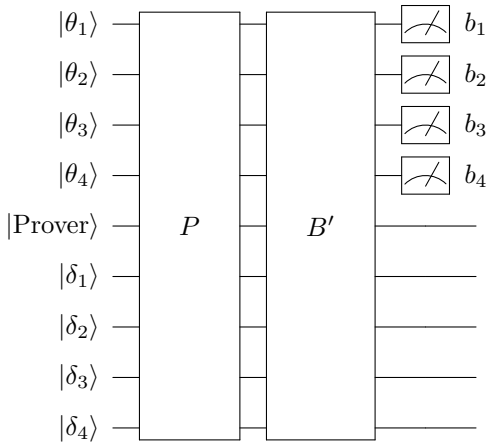


Here, $\{B_i\}$ are the individual operations performed by the prover and b_i is the outcome of a measurement always performed in the basis $\{|0\rangle, |1\rangle\}$. Without loss of generality we can assume that the measurement occurs immediately prior to transmission of each bit to the verifier, as shown above. Mathematically, the individual operations performed by the prover, $\{B_i\}$ can be combined into a single operation B, resulting in the quantum circuit shown below.

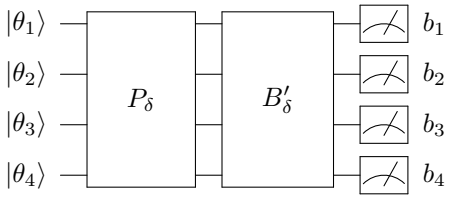


By defining $B' = BP^\dagger$, where P corresponds to the unitary implementing the protocol for an honest prover, the

circuit corresponding to the protocol can be rewritten as the ideal protocol followed by some deviation.



The verifier's output only corresponds to the measurement outputs received from the prover, and so the prover's effective deviation operator can be reduced to a super-operator, dependent on the specific values of $\{\delta_i\}$ used in that run of the protocol, acting only on these qubits.



As the left hand part of the above circuit implements the ideal protocol, B'_δ contains any error introduced by the prover.

Note that the output of the ideal protocol $b = \{b_i\}$ is the output of the verifier's chosen computation, $m = \{m_i\}$, bitwise xored with a random bitstring, $r = \{r_i\}$, known only to the verifier:

$$b = m \oplus r.$$

In the following, we encode the classical information in a quantum system:

$$\begin{aligned} b &\rightarrow |b\rangle, \\ m &\rightarrow |m\rangle, \\ r &\rightarrow |r\rangle, \text{and} \\ (m \oplus r) &\rightarrow |m \oplus r\rangle, \end{aligned}$$

thus n classical bits are encoded in n qubits.

Therefore, for a fixed computation chosen by the verifier with outcome m, on n qubits, the probability of an error occurring (averaging over all possible choices for the random bitstring r) is given by

$$\begin{aligned} \epsilon &= \frac{1}{2^n} \sum_{r \in \{0,1\}^n} \text{Tr}\left[\left(\mathbb{I}_{2^n} - |m+r\rangle\langle m+r|\right) B'_\delta \left(|m+r\rangle\langle m+r|\right)\right], \\ &= \frac{1}{2^n} \sum_{b \in \{0,1\}^n} \text{Tr}\left[\left(\mathbb{I}_{2^n} - |b\rangle\langle b|\right) B'_\delta \left(|b\rangle\langle b|\right)\right], \end{aligned}$$

for a fixed computation. Here, n is the number of qubits involved in the protocol and $\mathbb{I}_{2^n}$ is the 2^n-dimensional density matrix.

Note, however, that for a trap located on any measured qubit i for which the expected measurement outcome is r_i, the probability of the trap registering an error is:

$$t_{i,r_i} = \text{Tr}\left[\left(\mathbb{I}_{2^n} - \mathbb{I}_{2^{i-1}} \otimes |r_i\rangle\langle r_i| \otimes \mathbb{I}_{2^{n-i}}\right) B'_\delta \left(\frac{\mathbb{I}_{2^{i-1}}}{2^{i-1}} \otimes |r_i\rangle\langle r_i| \otimes \frac{\mathbb{I}_{2^{n-i}}}{2^{n-i}} \right) \right],$$

where $|r_i\rangle$ a 2-dimensional quantum state encoding the classical value r_i. Here, we use the fact that for a measurement of a trap qubit we expect $m_i = 0$, and thus $r_i = b_i$.

Averaging over all possible choices of i and r_i, this yields an average probability of detection of

$$\begin{aligned}\langle t\rangle &= \sum_{i=1}^{n}\frac{1}{n}\sum_{b\in\{0,1\}^n}\frac{1}{2^n}\mathrm{Tr}\left[\left(\mathbb{I}_{2^n}-\mathbb{I}_{2^{i-1}}\otimes|b_i\rangle\langle b_i|\otimes\mathbb{I}_{2^{n-i}}\right)B'_\delta\left(|b\rangle\langle b|\right)\right]\\ &= \frac{1}{n\,2^n}\sum_{b\in\{0,1\}^n}\mathrm{Tr}\left[\left(\sum_{i=1}^{n}\left(\mathbb{I}_{2^n}-\mathbb{I}_{2^{i-1}}\otimes|b_i\rangle\langle b_i|\otimes\mathbb{I}_{2^{n-i}}\right)\right)B'_\delta\left(|b\rangle\langle b|\right)\right],\end{aligned}$$

where $|b_i\rangle_i$ a 2-dimensional quantum state encoding the classical value b_i.

As the $B'_\delta\left(|b\rangle\langle b|\right)$ is positive semi-definite, and

$$\left(\mathbb{I}_{2^n}-|b\rangle\langle b|\right)\preceq\sum_{i=1}^{n}\left(\mathbb{I}_{2^n}-|b_i\rangle_i\langle b_i|_i\right),$$

then

$$\langle t\rangle\geq\frac{2^{-n}}{n}\sum_{b\in\{0,1\}^n}\mathrm{Tr}\left[\left(\mathbb{I}_{2^n}-|b\rangle\langle b|\right)B'_\delta\left(|b\rangle\langle b|\right)\right]$$

where b_i is the ith bit of b. Thus, by substituting in ϵ into the above equation and rearranging, we obtain $\epsilon\leq n\langle t\rangle$.

Traps prepared by MBQC

Contrary to the protocol described in [12], in the current experiment we rely on measurement-based computation to prepare isolated trap qubits (instead of preparing them directly). For example to prepare qubit 4 as a trap qubit, we choose a blind linear cluster state which implements the following computation:

$$|\mathrm{trap}_4\rangle = R_z\left(\theta_4\right)HR_z\left(m_3\pi\right)HR_z\left(\frac{\pi}{2}+m_2\pi\right)HR_z\left(\frac{\pi}{2}+m_1\pi\right)|+\rangle.$$

The output state $|\mathrm{trap}_4\rangle$ then depends on the outcomes of the measurement of qubit 1, 2 and 3 which are blind to the prover.

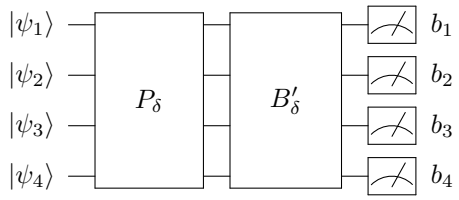
The general measurement patterns which can achieve such isolated trap qubits, together with the corresponding state of the trap qubit prepared are shown in Table I.

Trap qubit	Measurements				Trap state
	1	2	3	4	
1		σ	Y	Y	$\|+_{(m_3\oplus m_4)\pi}\rangle$
2	Y		X	Y	$\|+_{(m_1\oplus m_3\oplus m_4)\pi}\rangle$
3	Y	X		Y	$\|+_{(m_1\oplus m_2\oplus m_4)\pi}\rangle$
4	Y	Y	σ		$\|+_{(m_1\oplus m_2)\pi}\rangle$

TABLE I: Measurement choices for non-trap qubits which prepare isolated trap qubits at each location. Note that if the choice of measurement operator for a given qubit does not affect the outcome then the measurement has been denoted by σ.

In order to determine the affect of a cheating prover, it is convenient to note that each of these trap measurements can also be interpreted as a stabilizer measurement of the underlying cluster state, as shown in Table II. Table III gives the cluster state measurement angles ϕ and sample corresponding pairs of blind state preparation and measurement angles (θ, δ), together with the classical computation performed in each case to verify the outcome of the trap measurement.

As in the previous section, a general deviation by the prover can be modeled by the quantum circuit below.



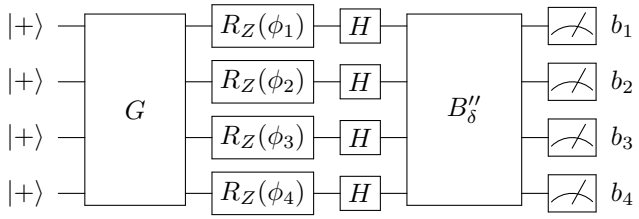
Trap qubit	Stabilizer
1	$X \otimes \mathbb{I} \otimes Y \otimes Y$
2	$Y \otimes X \otimes X \otimes Y$
3	$Y \otimes X \otimes X \otimes Y$
4	$Y \otimes Y \otimes \mathbb{I} \otimes X$

TABLE II: Index of trap qubit and corresponding stabilizer measurement.

Trap qubit	ϕ				Sample (θ_i, δ_i)				Trap outcome
	1	2	3	4	1	2	3	4	
1	0	0	$\frac{\pi}{2}$	$\frac{\pi}{2}$	$(0,0)$	$\left(\frac{\pi}{2}, -\frac{\pi}{2}\right)$	$\left(\frac{3\pi}{4}, \frac{5\pi}{4}\right)$	$\left(0, \frac{\pi}{2}\right)$	$m_1 \oplus m_3 \oplus m_4$
2	$\frac{\pi}{2}$	0	0	$\frac{\pi}{2}$	$\left(0, \frac{\pi}{2}\right)$	$\left(\frac{\pi}{2}, \frac{\pi}{2}\right)$	$\left(\frac{3\pi}{4}, \frac{7\pi}{4}\right)$	$\left(0, \frac{\pi}{2}\right)$	$m_1 \oplus m_2 \oplus m_3 \oplus m_4$
3	$\frac{\pi}{2}$	0	0	$\frac{\pi}{2}$	$\left(0, \frac{\pi}{2}\right)$	$\left(\frac{\pi}{2}, \frac{\pi}{2}\right)$	$\left(\frac{3\pi}{4}, \frac{7\pi}{4}\right)$	$\left(0, \frac{\pi}{2}\right)$	$m_1 \oplus m_2 \oplus m_3 \oplus m_4$
4	$\frac{\pi}{2}$	$\frac{\pi}{2}$	0	0	$\left(0, -\frac{\pi}{2}\right)$	$\left(\frac{\pi}{2}, 0\right)$	$(\pi, 0)$	(0,0)	$m_1 \oplus m_2 \oplus m_4$

TABLE III: Measurement angle for each trap setting together with sample δ and θ. The trap outcome should be consistent with the equation in the right most column in the above table, and any discrepancy represents the detection of an error.

Equivalently this can be rewritten as



Here, the left hand portion of the circuit performs the unitary part of the ideal measurement-based computation, immediately prior to measurement in the computational basis, with G representing the entangling gate which generates the cluster state from separable qubits via a series of controlled-Z operations. The deviation operator B''_δ can be expanded as a sum over Kraus operators, $\{\chi^k_\delta\}$, acting on the density matrix.

Next, χ^k_δ can be expanded as a sum over 4-qubit Pauli operators (including the identity), $\{\sigma_i\}$, weighted by complex coefficients, so that $\chi^k_\delta = \sum w^k_i \sigma_i$, with $w^k_i \in \mathbb{C}$ and $\sum_k \sum_i w^k_i w^{k*}_i = 1$. Table IV shows whether a given Pauli term in the deviation operator commutes or anticommutes with each trap setting, and hence whether such an error is detectable or not. We note that the only Pauli terms which commute with the measurement and terms which correspond to a simultaneous bit-flip error on only the first and last qubits remain undetected. The first set of terms leave the computation unaltered, and hence do not represent errors. However the latter group do represent an error which cannot be detected by our current setup.

While this appears to be an insurmountable problem if we wish to verify a general quantum computation, the problem disappears entirely if we consider only those computations for which the output of the computation only depends on the parity of the measurement results of qubits 1 and 4. This is because flipping both measurement outcomes leaves their parity invariant, and hence the outcome of the computation remains the same. Thus for the remainder of this section we consider only those computations for which simultaneously flipping the first and last measurement results leave the outcome of the computation invariant.

With this restriction in place, we take the verification protocol to proceed as follows. First the verifier randomly chooses whether or not to perform a computation as normal or instead to perform a trap computation. We assume that a trap computation is chosen with probability p. Next the verifier chooses uniformly at random an index for the trap qubit. As traps 2 and 3 correspond to the same stabilizer measurement we would obtain a better probability of detecting an error by choosing between the three stabilizer measurements uniformly at random. However, here we

Pauli (σ_i)	Trap Stabilizer Measurement			Overall
	$X \otimes \mathbb{I} \otimes Y \otimes Y$	$Y \otimes X \otimes X \otimes Y$	$Y \otimes Y \otimes \mathbb{I} \otimes X$	
$C \otimes C \otimes C \otimes C$	✓	✓	✓	✓
$C \otimes C \otimes C \otimes A$	✗	✗	✗	✗
$C \otimes C \otimes A \otimes C$	✗	✗	✓	✗
$C \otimes C \otimes A \otimes A$	✓	✓	✗	✗
$C \otimes A \otimes C \otimes C$	✓	✗	✗	✗
$C \otimes A \otimes C \otimes A$	✗	✓	✓	✗
$C \otimes A \otimes A \otimes C$	✗	✓	✗	✗
$C \otimes A \otimes A \otimes A$	✓	✗	✓	✗
$A \otimes C \otimes C \otimes C$	✗	✗	✗	✗
$A \otimes C \otimes C \otimes A$	✓	✓	✓	✓
$A \otimes C \otimes A \otimes C$	✓	✓	✗	✗
$A \otimes C \otimes A \otimes A$	✗	✗	✓	✗
$A \otimes A \otimes C \otimes C$	✗	✓	✓	✗
$A \otimes A \otimes C \otimes A$	✓	✗	✗	✗
$A \otimes A \otimes A \otimes C$	✓	✗	✓	✗
$A \otimes A \otimes A \otimes A$	✗	✓	✗	✗

TABLE IV: Pauli terms in the deviation operator B''_δ and whether or not they are detected by a particular trap setup or not. Although there are 256 distinct 4-qubit Pauli operators, including the identity, these can be grouped into 16 distinct sets based on whether each local term commutes ($C \in \{\mathbb{I}, Z\}$) or anticommutes ($A \in \{X, Y\}$) with the computational basis measurement carried out immediately after the deviation operator acts. Note that all such terms are either leave the computation invariant, or are detected by at least one trap setting, with the exception of $A \otimes C \otimes C \otimes A$.

use an identical probability for choosing each trap index, since this is optimal in the case where our experimental restrictions are limited and we can employ the full protocol of [12].

We wish to bound the probability that a given run of the computation yields the correct results based on the probability of trap computations yielding incorrect results. To do this, we note that for the set of computations we consider, any Pauli term in B''_δ which leads to an error in the outcome of the computation necessarily anticommutes with at least one of the trap stabilizer measurements and hence is detected with probability at least $p/4$. Thus any deviation which flips at least one of the measurement outcomes is detected with probability at least $p/4$. If the probability that a malicious prover flips one or more measurement outcomes is ϵ, then the probability that a trap computation yields the correct result is $\langle t \rangle \geq \epsilon p/4$. Thus the probability that the outcome of a computation is incorrect is bounded from above by $\epsilon \leq \frac{4\langle t \rangle}{p}$.

We note that in order for the above verification procedure to work, it is necessary for all qubits to be fully blind (i.e. all possible choices of θ and δ from $\{0, \frac{\pi}{4}, \frac{\pi}{2}, \frac{3\pi}{4}, \pi, \frac{5\pi}{4}, \frac{3\pi}{2}, \frac{7\pi}{4}\}$ should be possible for each qubit). In the current generation of experiments this property holds only for qubits 2 and 3, and the value for δ_1 and δ_4 are fixed. However we note that these fixed values do represent a legitimate choice on the part of the verifier, and as long as the prover does not have a priori information about this restriction the proof of authentication holds.

Experimental settings

In our experiment, we choose the set of phases and measurement setting as given in Table V to prepare traps on all qubits:

ENTANGLEMENT VERIFICATION

As discussed in the main paper we demonstrate how our restricted verification scheme can be exploited for the verification of a non-classical computation, in the form of a measurement of Bell statistics. For a test of Bell's inequality, the certain measurements α, α' and β, β' need to be performed on a two-qubit state $|\psi\rangle_{a,b}$, where α, α' (β, β') are the measurements performed on qubit a (b). If the state $|\psi\rangle_{a,b}$ is entangled, a maximal violation of the

$\|\text{trap}_1\rangle = \|-_i\rangle$:	$\theta_1 = 0$, $\theta_2 = \pi/2$, $\theta_3 = 0$, $\theta_4 = 0$ $\delta_1 = \delta_{\text{trap}}$, $\delta_2 = -\pi/2$, $\delta_3 = \pi$, $\delta_4 = -\pi/2$
$\|\text{trap}_1\rangle = \|+\rangle$:	$\theta_1 = 0$, $\theta_2 = \pi/2$, $\theta_3 = 3\pi/2$, $\theta_4 = 0$ $\delta_1 = \delta_{\text{trap}}$, $\delta_2 = -\pi/2$, $\delta_3 = 5\pi/4$, $\delta_4 = \pi/2$
$\|\text{trap}_2\rangle = \|+\rangle$:	$\theta_1 = 0$, $\theta_2 = \pi/2$, $\theta_3 = \pi$, $\theta_4 = 0$ $\delta_1 = -\pi/2$, $\delta_2 = \delta_{\text{trap}}$, $\delta_3 = 0$, $\delta_4 = 0$
$\|\text{trap}_2\rangle = \|+_i\rangle$:	$\theta_1 = 0$, $\theta_2 = 0$, $\theta_3 = 0$, $\theta_4 = 0$ $\delta_1 = \pi/2$, $\delta_2 = \delta_{\text{trap}}$, $\delta_3 = 0$, $\delta_4 = 0$
$\|\text{trap}_3\rangle = R_z(3\pi/4)\|+\rangle$:	$\theta_1 = 0$, $\theta_2 = \pi/2$, $\theta_3 = 5\pi/4$, $\theta_4 = 0$ $\delta_1 = \pi$, $\delta_2 = -\pi/2$, $\delta_3 = \delta_{\text{trap}}$, $\delta_4 = \pi/2$
$\|\text{trap}_3\rangle = R_z(\pi/4)\|+\rangle$:	$\theta_1 = 0$, $\theta_2 = \pi/2$, $\theta_3 = 7\pi/4$, $\theta_4 = 0$ $\delta_1 = \pi$, $\delta_2 = 0$, $\delta_3 = \delta_{\text{trap}}$, $\delta_4 = -\pi/2$
$\|\text{trap}_4\rangle = \|-\rangle$:	$\theta_1 = 0$, $\theta_2 = \pi/2$, $\theta_3 = \pi/4$, $\theta_4 = 0$ $\delta_1 = \pi/2$, $\delta_2 = 0$, $\delta_3 = 5\pi/4$, $\delta_4 = \delta_{\text{trap}}$
$\|\text{trap}_4\rangle = \|-_i\rangle$:	$\theta_1 = 0$, $\theta_2 = \pi/2$, $\theta_3 = 3\pi/4$, $\theta_4 = 0$ $\delta_1 = \pi/2$, $\delta_2 = \pi/2$, $\delta_3 = 7\pi/4$, $\delta_4 = \delta_{\text{trap}}$

TABLE V: Blind phases and measurement instructions for the entanglement verification procedure.

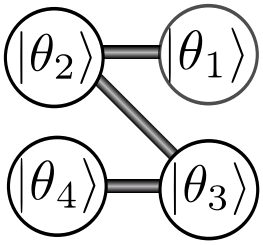


FIG. 5: Blind zigzag cluster

Bell inequality of the Clauser-Horne-Shimony-Holt (CHSH)-type,

$$S = |E(\alpha, \beta) - E(\alpha, \beta')| + |E(\alpha', \beta) + E(\alpha', \beta')| \leq 2, \tag{16}$$

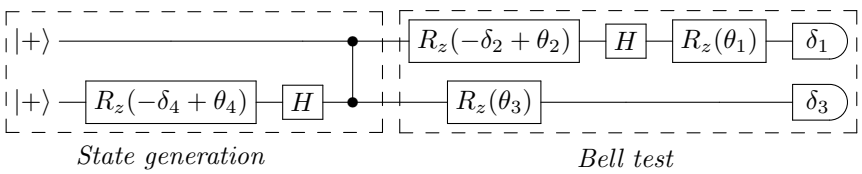
can be obtained. Here the correlation coefficients are defined as

$$E(\alpha, \beta) = \frac{C_{00}(\alpha, \beta) - C_{01}(\alpha, \beta) - C_{10}(\alpha, \beta) + C_{11}(\alpha, \beta)}{C_{00}(\alpha, \beta) + C_{01}(\alpha, \beta) + C_{10}(\alpha, \beta) + C_{11}(\alpha, \beta)} \tag{17}$$

and $C_{ij}(\alpha, \beta)$ are the coincidence counts for obtaining measurement results $i = \{0, 1\}$ on qubit a and $j = \{0, 1\}$ on qubit b for measurements in bases α and β on qubits a and b respectively.

We exploit the framework of blind quantum computing, in order to enable a verifier to perform a blind Bell test. We choose the blind cluster state to be a zigzag cluster state, shown in Figure 5.

The underlying circuit, which is obtained, when measurements in the basis $|\pm_{\delta_j}\rangle = (|0\rangle \pm e^{i\delta_j}|1\rangle)/\sqrt{2}$ are performed on the blind zigzag cluster state with blind qubits being in the state $|\theta_j\rangle$ is given by the circuit below

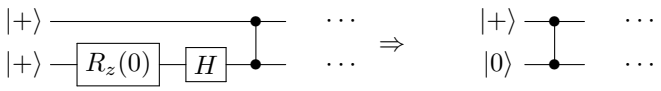


(18)

where —•— denotes a CPhase gate (CPhase$|ij\rangle = (-1)^{ij}|ij\rangle$) and —[$\phi$]— a measurement in the basis $|+_\phi\rangle$. Here, $R_z(\phi) = \exp(-i\phi\sigma_z/2)$, $H = (\sigma_x + \sigma_z)/\sqrt{2}$ and σ_x, σ_y and σ_z denote the usual Pauli matrices.

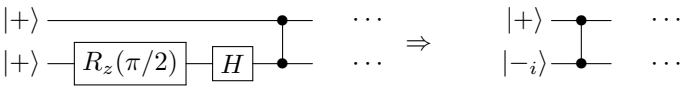
As we will see in the following, a blind Bell test can be implemented by choosing suitable combinations of δ_j and θ_j. For this, the left part of the circuit (shown above) implements the state generation, whereas the right parts realizes the Bell test.

The verifier can choose between entangled states and product states for the Bell test. For example, by choosing $-\delta_4 + \theta_4 = 0$ (or π), the input state will be a product state:



(19)

Alternatively, by choosing $-\delta_4 + \theta_4 = \pi/2$ (or $-\pi/2$), the input state will be an entangled state:



(20)

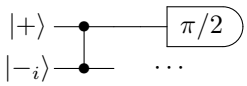
This demonstrates that the verifier can choose between different—product or entangled—input states for the Bell test by choosing different combinations of δ_4 and θ_4. For our demonstration, we exemplarily choose the entangled state to be CPhase$|+\rangle|-_i\rangle$.

In the blind framework, the Bell measurements are determined by the choice of the blind phases θ_1, θ_2, and θ_3 as well as by the measurement settings δ_1, δ_2, and δ_3 on the blind zigzag cluster state. For our demonstration, we choose the Bell measurement angles as given in the main paper.

The Bell settings of α and α' are determined by the choice of $(-\delta_2 + \theta_2)$ and $(\delta_1 - \theta_1)$. For the Bell measurement angle $\alpha = \pi/2$, we choose $\delta_1 - \theta_1 = \pi/2$ and $-\delta_2 + \theta_2 = \pi$.

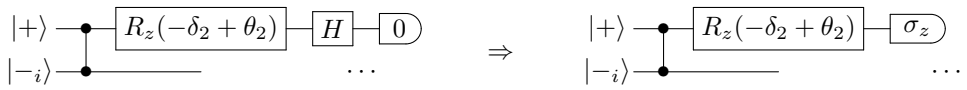
(21)

which leads to a measurement in the basis $\alpha = \pi/2$ in the upper wire:



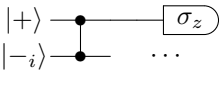
(22)

For the Bell measurement angle $\alpha' = \sigma_z$, we choose $\delta_1 - \theta_1 = 0$. With that configuration, $-\delta_2 + \theta_2$ can have any value, since a $R_z(-\delta_2 + \theta_2)$ rotation does not affect the state $|0\rangle$:



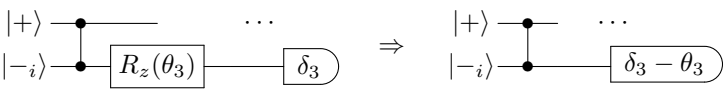
(23)

Finally, we obtain a measurement in the basis $\alpha' = \sigma_z$:



(24)

The angles β and β' are determined by δ_3 and θ_3.



(25)

To choose the Bell settings, $\beta = -3\pi/4$ and $\beta' = -\pi/4$, we simply take $\delta_3 - \theta_3$ to be equal to β or β'.

Experimental measurement settings

In our experiment, we choose the settings given in table VI.

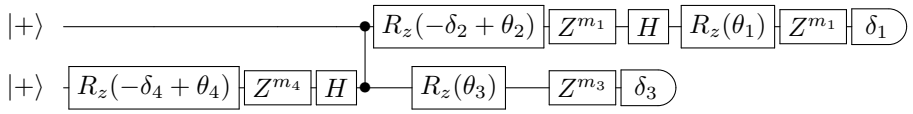
Note, that for the second setting α, β' we measure $\alpha + \pi$ and $\beta' + \pi$ instead of α and β'. This has no effect on the Bell inequality since only the measurement outcomes are exchanged ($00 \to 11$, $01 \to 10$, $10 \to 01$, $11 \to 00$). This exchange of the measurements outcomes can be interpreted as the verifier choosing $r_j = 1$. In the blind quantum computing framework, r_j is a randomly chosen value in $\{0, 1\}$ which hides the value of the measurement outcome.

α, β:	$\theta_1 = 0$, $\theta_2 = \pi/2$, $\theta_3 = 3\pi/4$, $\theta_4 = 0$ $\delta_1 = \pi/2$, $\delta_2 = -\pi/2$, $\delta_3 = 0$, $\delta_4 = -\pi/2$
α, β':	$\theta_1 = 0$, $\theta_2 = 0$, $\theta_3 = 3\pi/4$, $\theta_4 = 0$ $\delta_1 = \pi/2$, $\delta_2 = 0$, $\delta_3 = -\pi/2$, $\delta_4 = -\pi/2$
α',β:	$\theta_1 = 0$, $\theta_2 = \pi/2$, $\theta_3 = \pi/4$, $\theta_4 = 0$ $\delta_1 = 0$, $\delta_2 = -\pi/2$, $\delta_3 = -\pi/2$, $\delta_4 = -\pi/2$
α', β':	$\theta_1 = 0$, $\theta_2 = 0$, $\theta_3 = \pi/4$, $\theta_4 = 0$ $\delta_1 = 0$, $\delta_2 = 0$, $\delta_3 = 0$, $\delta_4 = -\pi/2$

TABLE VI: Blind phases and measurement instructions for the preparation of a set of trap qubits

Bell test verification

In order to show that the Bell test is invariant under errors of the form $A \otimes C \otimes C \otimes A$, as required to show verification in our setting, we note that the circuit implemented by our measurement settings is described by the circuit below.



Note that an error of this form flips both m_1 and m_4. The effect of flipping m_1 is trivially identical to flipping the outcome of the first logical qubit in the Bell test. Although it is not immediately obvious, we note that since $Z^{m_1}R_Z(-\delta_4+\theta_4) = R_Z(\pm\frac{\pi}{2})$ and $HZR_Z(\pm\frac{\pi}{2})|+\rangle = ZHR_Z(\pm\frac{\pi}{2})|+\rangle$, a bit flip error on m_4 leads to a bit flip error in the outcome of the measurement result for the second logical qubit. Thus all errors of the form $A \otimes C \otimes C \otimes A$ flip the outcome of both measurements in a Bell test. However, we note that the outcome of the Bell test depends only on the parity of these two measurements, and hence any inferred value of the CHSH quantity is left unchanged by such errors.